(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－69137

(43)公開日　平成11年(1999)３月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	1/387		Ｈ０４Ｎ	1/387	
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ａ
		６６０			６６０Ｄ
	5/00			5/00	
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ

審査請求　未請求　請求項の数15　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平9－223930

(22)出願日　平成９年(1997)８月20日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

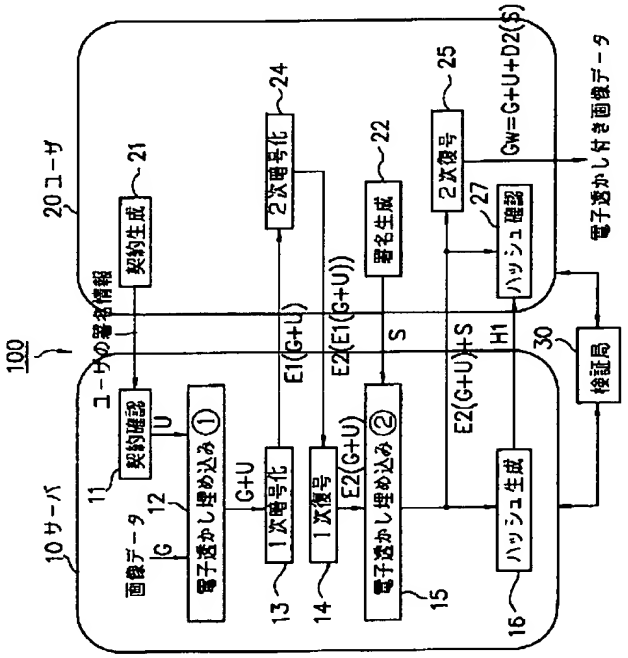
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　電子透かし方式、電子情報配布システムおよび画像ファイル装置

(57)【要約】

【課題】　著作権に係るディジタルデータの不正コピーを確実に防止できる電子透かし方式を提供する。

【解決手段】　複数のエンティティ間で送受信されるディジタル情報（画像データＧ）に対して電子透かし情報の埋め込み処理を行うエンティティ（サーバ端末装置１０）と、暗号処理を行うエンティティ（ユーザ端末装置２０）とを別に設けることにより、サーバまたはユーザがディジタルデータを不正にコピーして配布を行った際にその不正行為を確実に認識することができるようにする。また、このシステムでは、サーバとユーザの利害は相反するので、両者が結託して不正することはあり得ず、ディジタルデータの不正配布に関して安全なシステムを実現できる。



1

【特許請求の範囲】

【請求項１】　電子透かし情報の埋め込まれたデータに対して少なくとも暗号化および復号の一方の処理を行うことを特徴とする電子透かし方式。

【請求項２】　電子透かし情報が埋め込まれ、且つ、暗号化されたデータに対して、別の情報を更に電子透かし情報として埋め込むことを特徴とする電子透かし方式。

【請求項３】　上記別の情報を更に電子透かし情報として埋め込むデータは、上記電子透かし情報が埋め込まれた状態で暗号化されていることを特徴とする請求項２に記載の電子透かし方式。

【請求項４】　上記暗号化とは異なる暗号化を施した後上記別の情報を更に電子透かし情報として埋め込むことを特徴とする請求項２または３に記載の電子透かし方式。

【請求項５】　共通のデータに対して暗号化を行う前と、当該暗号化を行う後に、互いに異なる情報をそれぞれ電子透かし情報として埋め込むことを特徴とする電子透かし方式。

【請求項６】　複数のエンティティを含むネットワークシステムで用いられる電子透かし方式であって、
上記複数のエンティティ間で送受信される暗号化されたデータに対して電子透かしを埋め込むエンティティと、
上記暗号処理およびそれに対応する復号処理を実行するエンティティとを別に有することを特徴とする電子透かし方式。

【請求項７】　上記データが画像データであることを特徴とする請求項１～６の何れか１項に記載の電子透かし方式。

【請求項８】　複数のエンティティからなるネットワークシステム上でディジタル情報の送受信を行う電子情報配布システムにおいて、
上記ディジタル情報に対して電子透かし情報の埋め込み処理を行う第１のエンティティと、
上記ディジタル情報に対して暗号処理およびそれに対応する復号処理を行う第２のエンティティとを有することを特徴とする電子情報配布システム。

【請求項９】　複数のエンティティからなるネットワークシステムにおいて、第１のエンティティと第２のエンティティとがディジタル情報の送受信を行う場合、
上記第１のエンティティは、上記第２のエンティティにより暗号化された情報を受け取り、電子透かし情報の埋め込み処理を行って上記第２のエンティティに送信し、
上記第２のエンティティは、上記第１のエンティティより受け取った情報に上記暗号化に対する復号処理を行うことを特徴とする電子情報配布システム。

【請求項１０】　複数のエンティティからなるネットワークシステムにおいて、第１のエンティティと第２のエンティティとがディジタル情報の送受信を行う場合、
上記第１のエンティティは、第１の暗号化の前に電子透かし情報の埋め込み処理を行って、得られた情報を上記第２のエンティティに送信し、
上記第２のエンティティは、上記第１のエンティティより受け取った情報に第２の暗号化を行って、得られた情報を上記第１のエンティティに送信し、
上記第１のエンティティは、上記第２のエンティティより受け取った情報に対して上記第１の暗号化に対する第１の復号処理を行った後に電子透かし情報の埋め込み処理を行って、得られた情報を上記第２のエンティティに送信し、
上記第２のエンティティは、上記第１のエンティティより受け取った情報に対して上記第２の暗号化に対する第２の復号処理を行うことを特徴とする電子情報配布システム。

【請求項１１】　上記第１のエンティティが埋め込む電子透かし情報は、上記第２のエンティティに関する情報を含むことを特徴とする請求項８～１０の何れか１項に記載の電子情報配布システム。

【請求項１２】　上記第１のエンティティが埋め込む電子透かし情報は、送信するディジタル情報に関する情報を含むことを特徴とする請求項８～１１の何れか１項に記載の電子情報配布システム。

【請求項１３】　上記第１のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第２のエンティティの署名を検証することを特徴とする請求項８～１２の何れか１項に記載の電子情報配布システム。

【請求項１４】　暗号化されていた画像情報を復号して得た画像情報と、暗号化された状態で付加され上記画像情報と共に復号処理の施された電子透かし情報とを画像データとして格納することを特徴とする画像ファイル装置。

【請求項１５】　上記画像データとは別途、上記暗号化に係わる鍵情報を格納することを特徴とする請求項１４に記載の画像ファイル装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は電子透かし方式、電子情報配布システムおよび画像ファイル装置に関し、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のディジタル情報における著作権を保護するための電子透かし技術、それを用いてディジタル情報の配布を行うマルチメディアネットワークおよびそれを用いた画像ファイル装置に用いて好適なものである。

【０００２】

【従来の技術】近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。そこで取引される商品として、例えば画像

等を含むディジタルデータが考えられる。しかし、ディジタルデータは、完全なコピーを容易かつ大量に作成できるという性質を持ち、これは、そのディジタルデータを買ったユーザがオリジナルと同質のコピーを不正に作成して再配布できるという可能性を示す。これにより、本来ディジタルデータの著作者または著作者から正当に販売を委託された者（以下、「販売者」と言う）に支払われるべき代価が支払われず、著作権が侵害されていると考えられる。

【０００３】一方、著作者または販売者（以下、これらのディジタルデータを正当に配布する者をまとめて「サーバ」と言う）がユーザにディジタルデータを一度送ってしまうと、上述の不正コピーを完全に防止することはできない。そのため、不正コピーを直接防止するのではなく、電子透かしと呼ばれる手法が提案されている。この電子透かしとは、オリジナルのディジタルデータにある操作を加え、ディジタルデータに関する著作権情報やユーザに関する利用者情報をディジタルデータ中に埋め込むことによって、不正コピーが見つかった場合に誰がデータを再配布したのかを特定する手法である。

【０００４】従来の電子透かしを用いたシステムでは、サーバは完全に信頼できる機関であることが前提となっている。よって、もしサーバが信頼できる機関ではなく不正を行う可能性があるとすると、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう場合が存在する。

【０００５】これは、図１０に示すように、従来のシステムでは、ユーザを特定するための利用者情報ｄ１をディジタルデータ（以下、ディジタルデータを画像データとして説明する）ｇにサーバが埋め込むので、サーバが勝手に利用者情報ｄ１を埋め込んでそのコピーを不正に配布した場合、その利用者情報ｄ１から特定されるユーザ（図１０の例ではユーザU）は、サーバの主張を退ける手段がないためである。

【０００６】その対策として、例えば、「B.Pfitmann and M.Waidner："Asymmetic Fingerprinting,"EUROCRYPT'96」の文献（以下、文献１と言う）に、公開鍵暗号方式を用いたシステム（図１１）が提案されている。ここで、公開鍵暗号方式とは、暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。その代表例として、ＲＳＡ暗号やＥ１Ｇａｍａ１暗号等が知られている。以下、公開鍵暗号方式における（ａ）特徴、（ｂ）秘密通信や認証通信等のプロトコルについて述べる。

【０００７】（ａ）公開鍵暗号の特徴

（１）暗号鍵と復号鍵とが異なり、暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（２）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（３）送られてきた通信文の送信者が偽者でないこと、およびその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【０００８】（ｂ）公開鍵暗号のプロトコル

例えば、通信文Ｍに対して、公開の暗号鍵ｋｐを用いて行う暗号化操作をＥ（ｋｐ，Ｍ）とし、秘密の復号鍵ｋｓを用いて行う復号操作をＤ（ｋｓ，Ｍ）とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。

（１）暗号鍵ｋｐが与えられたとき、暗号化操作Ｅ（ｋｐ，Ｍ）の計算は容易である。また、復号鍵ｋｓが与えられたとき、復号操作Ｄ（ｋｓ，Ｍ）の計算は容易である。

（２）もしユーザが復号鍵ｋｓを知らないなら、暗号鍵ｋｐと、暗号化操作Ｅ（ｋｐ，Ｍ）の計算手順と、暗号文Ｃ＝Ｅ（ｋｐ，Ｍ）とを知っていても、通信文Ｍを決定することは計算量の点で困難である。

【０００９】次に、上記（１）、（２）の条件に加えて、次の（３）の条件が成立することにより秘密通信機能が実現できる。

（３）全ての通信文（平文）Ｍに対し暗号化操作Ｅ（ｋｐ，Ｍ）が定義でき、

Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））＝Ｍ

が成立する。つまり、暗号鍵ｋｐは公開されているため、誰もが暗号化操作Ｅ（ｋｐ，Ｍ）の計算を行うことができるが、Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））の計算をして通信文Ｍを得ることができるのは、秘密の復号鍵ｋｓを持っている本人だけである。

【００１０】一方、上記（１）、（２）の条件に加えて、次の（４）の条件が成立することにより認証通信機能が実現できる。

（４）全ての通信文（平文）Ｍに対し復号操作Ｄ（ｋｓ，Ｍ）が定義でき、

Ｅ（ｋｐ，Ｄ（ｋｓ，Ｍ））＝Ｍ

が成立する。つまり、復号操作Ｄ（ｋｓ，Ｍ）の計算ができるのは秘密の復号鍵ｋｓを持っている本人のみであり、他の人が偽の秘密の復号鍵ｋｓ'を用いてＤ（ｋｓ'，Ｍ）の計算を行い、秘密の復号鍵ｋｓを持っている本人になりすましたとしても、

Ｅ（ｋｐ，Ｄ（ｋｓ'，Ｍ）≠Ｍ

であるため、受信者は受けとった情報が不正なものであることを確認できる。また、Ｄ（ｋｓ，Ｍ）の値が改ざんされても、

Ｅ（ｋｐ，Ｄ（ｋｓ，Ｍ）'）≠Ｍ

となり、受信者は受けとった情報が不正なものであることを確認できる。

【００１１】上述のような公開鍵暗号方式では、公開の暗号鍵（以下、公開鍵とも言う）ｋｐを用いる処理Ｅ()を「暗号化」、秘密の復号鍵（以下、秘密鍵とも言う）ｋｓを用いる処理Ｄ()を「復号」と呼んでいる。したが

って、秘密通信では送信者が暗号化を行い、その後受信者が復号を行うが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【００１２】以下に、公開鍵暗号方式により送信者Ａから受信者Ｂへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。ここで、送信者Ａの秘密鍵をｋｓＡ、公開鍵をｋｐＡとし、受信者Ｂの秘密鍵をｋｓＢ、公開鍵をｋｐＢとする。

【００１３】[秘密通信]送信者Ａから受信者Ｂへ通信文（平文）Ｍを秘密通信する場合は、次の手順で行う。

Step１：送信者Ａは、受信者Ｂの公開鍵ｋｐＢで通信文Ｍを以下のように暗号化し、暗号文Ｃを受信者Ｂに送る。

Ｃ＝Ｅ（ｋｐＢ，Ｍ）

Step２：受信者Ｂは、自分の秘密鍵ｋｓＢで暗号文Ｃを以下のように復号し、もとの平文Ｍを得る。

Ｍ＝Ｄ（ｋｓＢ，Ｃ）

なお、受信者Ｂの公開鍵ｋｐＢは不特定多数に公開されているので、送信者Ａに限らず全ての人が受信者Ｂに秘密通信できる。

【００１４】[認証通信]送信者Ａから受信者Ｂへ通信文（平文）Ｍを認証通信する場合は、次の手順で行う。

Step１：送信者Ａは、自分の秘密鍵ｋｓＡで送信文Ｓを以下のように生成し、受信者Ｂに送る。

Ｓ＝Ｄ（ｋｓＡ，Ｍ）

この送信文Ｓを「署名文」と言い、署名文Ｓを得る操作を「署名」と言う。

Step２：受信者Ｂは、送信者Ａの公開鍵ｋｐＡで署名文Ｓを以下のように復元変換し、もとの平文Ｍを得る。

Ｍ＝Ｅ（ｋｐＡ，Ｓ）

もし、通信文Ｍが意味のある文であることを確認したならば、通信文Ｍが確かに送信者Ａから送られてきたことを認証する。送信者Ａの公開鍵ｋｐＡは不特定多数に公開されているので、受信者Ｂに限らず全ての人が送信者Ａの署名文Ｓを認証できる。このような認証を「ディジタル署名」とも言う。

【００１５】[署名付秘密通信]送信者Ａから受信者Ｂへ通信文（平文）Ｍを署名付秘密通信する場合は、次の手順で行う。

Step１：送信者Ａは、自分の秘密鍵ｋｓＡで通信文Ｍを以下のように署名し、署名文Ｓを作る。

Ｓ＝Ｄ（ｋｓＡ，Ｍ）

さらに、送信者Ａは、受信者Ｂの公開鍵ｋｐＢで署名文Ｓを以下のように暗号化し、暗号文Ｃを受信者Ｂに送る。

Ｃ＝Ｅ（ｋｐＢ，Ｓ）

Step２：受信者Ｂは、自分の秘密鍵ｋｓＢで暗号文Ｃを以下のように復号し、署名文Ｓを得る。

Ｓ＝Ｄ（ｋｓＢ，Ｃ）

さらに、受信者Ｂは、送信者Ａの公開鍵ｋｐＡで署名文

Ｓを以下のように復元変換し、もとの平文Ｍを得る。

Ｍ＝Ｅ（ｋｐＡ，Ｓ）

もし、通信文Ｍが意味のある文であることを確認したならば、通信文Ｍが確かに送信者Ａから送られてきたことを認証する。

【００１６】なお、署名付秘密通信の各Step内における関数を施す順序は、それぞれ逆転しても良い。すなわち、上述の手順では、

Step１：Ｃ＝Ｅ（ｋｐＢ，Ｄ（ｋｓＡ，Ｍ））

Step２：Ｍ＝Ｅ（ｋｐＡ，Ｄ（ｋｓＢ，Ｃ））

となっているが、下記のような手順でも署名付秘密通信が実現できる。

Step１：Ｃ＝Ｄ（ｋｓＡ，Ｅ（ｋｐＢ，Ｍ））

Step２：Ｍ＝Ｄ（ｋｓＢ，Ｅ（ｋｐＡ，Ｃ））

【００１７】以下に、上述のような公開鍵暗号方式を適用した従来の電子透かしを用いるシステム（上記図１１）における操作の手順を示す。

１）まず、サーバとユーザ間で画像データｇの売買に関する契約書ｄ２を取り交わす。

【００１８】２）次に、ユーザは、自分を示す乱数ＩＤを発生させ、これを用いて一方向性関数ｆを生成する。この一方向性関数とは、関数ｙ＝ｆ（ｘ）において、ｘからｙを求めることは容易だが、逆にｙからｘを求めることが困難な関数を言う。例えば、桁数の大きな整数に対する素因数分解や離散的対数等が一方向性関数としてよく用いられる。

３）次に、ユーザは、契約書ｄ２と一方向性関数ｆに対して、自分の秘密鍵ｋｓＵを用いて署名情報ｄ３を生成し、それらを合わせてサーバに送る。

【００１９】４）次に、サーバは、ユーザの公開鍵ｋｐＵを用いて署名情報ｄ３と契約書ｄ２を確認する。

５）サーバは確認後、現在までの全配布記録ｄ４と、ユーザが作成した乱数ＩＤとを画像データｇに埋め込み、電子透かし付き画像データ（ｇ＋ｄ４＋ＩＤ）を生成する。

６）サーバは、ユーザにその電子透かし付き画像データ（ｇ＋ｄ４＋ＩＤ）を送る。

【００２０】この後、不正コピーが発見された場合は、その不正画像データから埋め込み情報を抽出し、そこに含まれるＩＤからユーザを特定する。このとき、その不正コピーがサーバによって無断で配布されたものでないことは、以下のことを根拠として主張される。それは、ユーザを特定するＩＤはユーザ自身によって生成され、それを用いた一方向性関数値ｆにユーザの署名が付けられるので、サーバは任意のユーザに対してそのようなＩＤを生成できないということである。しかし、サーバとの間で正式に契約したユーザは自分を特定するＩＤをサーバに送るために、正式に契約したユーザへの罪の押し付けはやはり可能であり、契約していないユーザへの罪の押し付けが不可能になるだけである。

【００２１】そこで、正式に契約したユーザにも罪の押し付けが不可能になるシステム（図１２）が、「三浦，渡辺，嵩（奈良先端大）：“サーバの不正も考慮した電子透かしについて”，SCIS97-31C」の文献（以下、文献２と言う）に提案されている。これは、サーバを原画像サーバと埋め込みサーバに分割することによって実現される。ただし、このシステムでは、暗号化時および復号時において、埋め込まれた電子透かしは壊されないとしている。以下、上記図１２のシステムにおける操作の手順を示す。

【００２２】１）まず、ユーザが原画像サーバに所望の画像データを、署名ｄ５を付けて要求する。

２）原画像サーバは、その要求内容をユーザの署名ｄ５から確認し、その確認後に、要求された画像データｇを暗号化して埋め込みサーバに送る。このとき、原画像サーバは、ユーザ名ｕおよび委託内容ｄ６に対する署名を付けて埋め込みサーバに送る。これと同時に、原画像サーバは、暗号化に対する復号関数ｆ’をユーザに送る。

【００２３】３）埋め込みサーバは、送られてきた暗号化画像データｇ’と、署名（ｕ＋ｄ６）とを確認し、ユーザ名ｕおよび委託内容ｄ６を基にユーザを特定する利用者情報ｄ７の作成および埋め込みを行い、電子透かし付き暗号化画像データ（ｇ’＋ｄ７）を作成する。その後、埋め込みサーバは、その電子透かし付き暗号化画像データ（ｇ’＋ｄ７）をユーザに送る。

４）ユーザは、原画像サーバから送られてきた復号関数ｆ’を用いて、電子透かし付き暗号化画像データ（ｇ’＋ｄ７）を電子透かし付き画像データ（ｇ＋ｄ７）へと復号する。

【００２４】この後、不正コピーが発見された場合は、原画像サーバはその不正画像データを暗号化して埋め込み情報を抽出し、それを埋め込みサーバに送る。埋め込みサーバは、この埋め込み情報からユーザを特定する。このシステムでは、原画像サーバはユーザを特定するための利用者情報ｄ７を画像データｇに埋め込んでおらず、また、埋め込みサーバは復号関数ｆ’を知らない（画像を元に戻せない）ので、正式に契約したユーザに対しても、各サーバはユーザの利用者情報ｄ７を無断で埋め込んだ画像データを不正配布できないことを根拠にしている。

【００２５】しかしながら、この図１２のシステムでは、原画像サーバと埋め込みサーバとの結託については考慮せず、埋め込みサーバとユーザとの結託も考えていない。よって、埋め込みサーバが原画像である画像データｇの暗号化画像データｇ’を持ち、ユーザが復号関数ｆ’を持つため、原画像サーバと埋め込みサーバとが結託した場合には、上述の図１１のシステムと同様にサーバの不正が可能であるし、埋め込みサーバとユーザとが結託した場合には、原画像の不正入手が可能である。

【００２６】また、原画像サーバは復号関数ｆ’をユーザに送るが、ユーザの復号関数ｆ’の管理が不十分であれば、埋め込みサーバはユーザと結託しなくてもユーザの不注意等から復号関数ｆ’を知ることができる可能性は大きい。

【００２７】さらに、このシステムでは、原画像サーバは埋め込み手段を有しない、または正しい埋め込みができないとしているが、埋め込み情報を抽出するのは原画像サーバであるので、埋め込み情報を解析すれば、原画像サーバが正しい埋め込みを行えるようになる可能性は高いと考えられる。これは、埋め込みサーバは自分の署名などを埋め込まないので、埋め込み情報と利用者情報の対応のみが埋め込みサーバの秘密であるが、データベース等を用いた埋め込み情報と利用者情報のランダムな対応ではなく、ある規則に基づいて利用者情報から埋め込み情報が作成される場合、解析される危険性は大きいからである。そして、この場合、上述の図１１のシステムと同様の不正が可能である。

【００２８】

【発明が解決しようとする課題】本発明はこのような実情に鑑みて成されたものであり、上述のようなサーバおよびユーザの不正を確実に防止できる電子透かし方式および電子情報配布システムを提供することを目的とする。

【００２９】

【課題を解決するための手段】本発明の電子透かし方式は、電子透かし情報の埋め込まれたデータに対して少なくとも暗号化および復号の一方の処理を行うことを特徴とする。

【００３０】本発明の他の特徴とするところは、電子透かし情報が埋め込まれ、且つ、暗号化されたデータに対して、別の情報を更に電子透かし情報として埋め込むことを特徴とする。ここで、上記別の情報を更に電子透かし情報として埋め込むデータは、上記電子透かし情報が埋め込まれた状態で暗号化されているものであっても良い。また、上記暗号化とは異なる暗号化を施した後上記別の情報を更に電子透かし情報として埋め込むようにしても良い。

【００３１】本発明のその他の特徴とするところは、共通のデータに対して暗号化を行う前と、当該暗号化を行う後に、互いに異なる情報をそれぞれ電子透かし情報として埋め込むことを特徴とする。

【００３２】本発明のその他の特徴とするところは、複数のエンティティを含むネットワークシステムで用いられる電子透かし方式であって、上記複数のエンティティ間で送受信される暗号化されたデータに対して電子透かしを埋め込むエンティティと、上記暗号処理およびそれに対応する復号処理を実行するエンティティとを別に有することを特徴とする。以上の構成において、上記データは画像データであっても良い。

【００３３】また、本発明の電子情報配布システムは、

複数のエンティティからなるネットワークシステム上でディジタル情報の送受信を行う電子情報配布システムにおいて、上記ディジタル情報に対して電子透かし情報の埋め込み処理を行う第１のエンティティと、上記ディジタル情報に対して暗号処理およびそれに対応する復号処理を行う第２のエンティティとを有することを特徴とする。

【００３４】本発明の他の特徴とするところは、複数のエンティティからなるネットワークシステムにおいて、第１のエンティティと第２のエンティティとがディジタル情報の送受信を行う場合、上記第１のエンティティは、上記第２のエンティティにより暗号化された情報を受け取り、電子透かし情報の埋め込み処理を行って上記第２のエンティティに送信し、上記第２のエンティティは、上記第１のエンティティより受け取った情報に上記暗号化に対する復号処理を行うことを特徴とする。

【００３５】本発明のその他の特徴とするところは、複数のエンティティからなるネットワークシステムにおいて、第１のエンティティと第２のエンティティとがディジタル情報の送受信を行う場合、上記第１のエンティティは、第１の暗号化の前に電子透かし情報の埋め込み処理を行って、得られた情報を上記第２のエンティティに送信し、上記第２のエンティティは、上記第１のエンティティより受け取った情報に第２の暗号化を行って、得られた情報を上記第１のエンティティに送信し、上記第１のエンティティは、上記第２のエンティティより受け取った情報に対して上記第１の暗号化に対する第１の復号処理を行った後に電子透かし情報の埋め込み処理を行って、得られた情報を上記第２のエンティティに送信し、上記第２のエンティティは、上記第１のエンティティより受け取った情報に対して上記第２の暗号化に対する第２の復号処理を行うことを特徴とする。

【００３６】ここで、上記第１のエンティティが埋め込む電子透かし情報は、少なくとも上記第２のエンティティに関する情報および送信するディジタル情報に関する情報の一方を含むものであっても良い。

【００３７】また、ここで、好適には上記第１のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第２のエンティティの署名を検証するようにする。

【００３８】また、本発明の画像ファイル装置は、暗号化されていた画像情報を復号して得た画像情報と、暗号化された状態で付加され上記画像情報と共に復号処理の施された電子透かし情報とを画像データとして格納することを特徴とする。ここで、上記画像データとは別途、上記暗号化に係わる鍵情報を格納するようにしても良い。

【００３９】

【発明の実施の形態】

〔第１の実施形態〕以下、本発明に係る第１の実施形態を、図１を参照して説明する。本発明に係る電子透かし方式は、例えば、図１に示すようなシステム１００により実施され、このシステム１００は、本発明に係る電子情報配布システムを適用したものでもある。

【００４０】すなわち、システム１００は、サーバ側の端末装置（サーバ端末装置）１０、ユーザ側の端末装置（ユーザ端末装置）２０および検証局側の端末装置（検証局端末装置）３０を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにディジタルデータの授受を行うようになされている。

【００４１】サーバ端末装置１０は、ユーザ端末装置２０からのデータが供給される契約確認処理部１１と、例えば画像データ（ディジタルデータ）が供給される第１の電子透かし埋め込み処理部１２と、上記第１の電子透かし埋め込み処理部１２の出力が供給される１次暗号化処理部１３と、ユーザ端末装置２０からのデータが供給される１次復号処理部１４と、ユーザ端末装置２０からのデータおよび１次復号処理部１４の出力が供給される第２の電子透かし埋め込み処理部１５と、上記第２の電子透かし埋め込み処理部１５の出力が供給されるハッシュ生成処理部１６とを備えており、１次暗号化処理部１３およびハッシュ生成処理部１６の各出力がユーザ端末装置２０に送信されるようになされている。また、第２の電子透かし埋め込み処理部１５の出力は、ハッシュ生成処理部１６に供給されるとともに、ユーザ端末装置２０にも送信されるようになされている。

【００４２】また、ユーザ端末装置２０は、サーバ端末装置１０の契約確認処理部１１に対してデータ送信する契約生成処理部２１と、署名生成処理部２２と、サーバ端末装置１０の１次暗号化処理部１３からのデータが供給される２次暗号化処理部２４と、サーバ端末装置１０の第２の電子透かし埋め込み処理部１５からのデータが供給される２次復号処理部２５と、サーバ端末装置１０の１次復号処理部１４からのデータが供給される２次復号処理部２５と、サーバ端末装置１０の第２の電子透かし埋め込み処理部１５およびハッシュ生成処理部１６からのデータが供給されるハッシュ確認処理部２７とを備えており、２次復号処理部２５の出力が電子透かし付き画像データとして出力されるようになされている。また、２次暗号化処理部２４の出力は、サーバ端末装置１０の１次復号処理部１４に供給され、署名生成処理部２３の出力は、サーバ端末装置１０の第２の電子透かし埋め込み処理部１５に供給されるようになされている。

【００４３】上述のようなシステム１００では、方式や秘密鍵等の１次暗号に関する情報はサーバだけが知る情報であり、２次暗号に関する情報はユーザだけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下、暗号化を「E

ｉ（）」、復号を「Ｄｉ（）」で表わし、電子透かしに関する埋め込み処理を「＋」で表わすものとする。

【００４４】以下に、上記のように構成したシステム１００の動作を説明する。まず、電子透かしに関する埋め込み処理について説明する。

【００４５】[埋め込み処理]

１）まず、ユーザ端末装置２０において、ユーザが署名を付けてサーバ端末装置１０に所望の画像データを要求する。この要求データは、契約生成処理部２１により生成された情報（ユーザの署名情報）であり、以下ではこれを契約情報と呼ぶ。

【００４６】２）次に、サーバ端末装置１０において、契約確認処理部１１は、受信した契約情報をユーザの署名から確認し、その確認後に、契約情報から利用者情報Ｕを作成する。そして、第１の電子透かし埋め込み処理部１２は、上記契約確認処理部１１で作成された利用者情報Ｕを要求された画像データＧに埋め込む。また、１次暗号化処理部１３は、第１の電子透かし埋込処理部１２で利用者情報Ｕが埋め込まれた画像データ（Ｇ＋Ｕ）に対して１次暗号化処理Ｅ１()を行い、得られたデータをユーザ端末装置２０に送る。よって、ユーザ端末装置２０には、１次暗号化画像データＥ１（Ｇ＋Ｕ）の情報が送られることになる。

【００４７】３）次に、ユーザ端末装置２０において、２次暗号化処理部２４は、サーバ端末装置１０から送られてきた１次暗号化画像データＥ１（Ｇ＋Ｕ）に対して２次暗号化を行い、得られた２次暗号化画像データＥ２（Ｅ１（Ｇ＋Ｕ））をサーバ端末装置１０に送る。このとき、ユーザは、署名生成処理部２２により自分の秘密鍵を用いて署名情報Ｓを生成し、サーバ端末装置１０に送る。

【００４８】４）次に、サーバ端末装置１０において、１次復号処理部１４は、ユーザ端末装置２０から送られてきた２次暗号化画像データＥ２（Ｅ１（Ｇ＋Ｕ））の１次暗号化を復号する。また、第２の電子透かし埋め込み処理部１５は、同じくユーザ端末装置２０から送られてきた署名情報Ｓを確認し、確認した署名情報Ｓを、上記１次復号処理部１４で生成されたＥ２（Ｇ＋Ｕ）の情報に埋め込み、ユーザ端末装置２０に送る。また、ハッシュ生成処理部１６は、ユーザ端末装置２０への送信データＥ２（Ｇ＋Ｕ）＋Ｓに対するハッシュ値Ｈ１を生成および署名し、上記送信データＥ２（Ｇ＋Ｕ）＋Ｓと共にユーザ端末装置２０に送る。よって、ユーザ端末装置２０には、Ｅ２（Ｇ＋Ｕ）＋Ｓの情報とハッシュ値Ｈ１、およびその署名が送られることになる。

【００４９】なお、ハッシュ値とは、一般にハッシュ関数ｈ()の出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは、異なる値ｘ１，ｘ２に対してｈ（ｘ１）＝ｈ（ｘ２）となることである。また、圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは、任意のビット長のビット列をある長さのビット列に変換する関数ｈ()で、ｈ（ｘ１）＝ｈ（ｘ２）を満たす値ｘ１，ｘ２を容易に見出せないものである。このとき、任意の値ｙからｙ＝ｈ（ｘ）を満たす値ｘを容易に見出せないので、必然的にハッシュ関数は一方向性関数となる。このハッシュ関数の具体例としては、ＭＤ（Message Digest）５やＳＨＡ（Secure Hash Algorithm）等が知られている。

【００５０】５）次に、ユーザ端末装置２０において、ハッシュ確認処理部２７は、サーバ端末装置１０から送られてきたハッシュＨ１とその署名とを確認し、上記ハッシュ値Ｈ１と、Ｅ２（Ｇ＋Ｕ）＋Ｓの情報から生成されるハッシュ値とが一致することを確認する。そして、その確認後に上記Ｅ２（Ｇ＋Ｕ）＋Ｓの情報およびハッシュ値Ｈ１とその署名を保存する。さらに、２次復号処理部２５は、サーバ端末装置１０から送られてきたＥ２（Ｇ＋Ｕ）＋Ｓの情報の２次暗号化を復号して電子透かし付き画像データＧｗを取り出す。よって、電子透かし付き画像データＧｗは、Ｇｗ＝Ｇ＋Ｕ＋Ｄ２（Ｓ）と表わされる。これは、元の画像データＧに利用者情報Ｕと２次暗号の影響を受けた署名情報Ｓとが透かし情報として埋め込まれていることを示す。

【００５１】以上のように、本実施形態による電子透かし方式によれば、電子透かし情報の埋め込みは全てサーバ側で行うので、ユーザは基本的に不正をすることができない。サーバ側では、ユーザ側から署名情報Ｓを直接受け取ってそれを電子透かし情報として埋め込むが、上記埋め込み処理中の５）の変換手順によってユーザ端末装置２０で得られた署名情報Ｄ２（Ｓ）は、ユーザのみが知る２次暗号化の影響を受けたものであるので、サーバは署名情報Ｄ２（Ｓ）を直接原画像に埋め込んでユーザに罪を着せることはできない。

【００５２】そこで、不正コピー（不正画像）が発見された場合は、以下のような検証処理によって不正者の特定を行う。ただし、ここでは上述の文献１、文献２と同様に、画像データは透かし情報の変形および消去を受けないものとする。

【００５３】[検証処理]

１）まず、サーバ端末装置１０において、発見した不正画像Ｇｗ’＝Ｇ＋Ｕ’＋Ｄ２（Ｓ’）から利用者情報Ｕ’を抽出する。

２）サーバ端末装置１０は、不正画像ＧＷ’と抽出した利用者情報Ｕ’とを検証局３０に示し、ユーザへの検査を要求する。

３）検証局３０は、ユーザが保存している２次暗号の鍵の提出を求め、提出された暗号鍵を使って不正画像Ｇｗ’を２次暗号化することにより、署名情報Ｓ’の抽出を行う。

【００５４】４）ここで、正しい署名情報が抽出された

場合（Ｓ’＝Ｓの場合）には、ユーザの不正と認定する。

５）また、正しい署名情報が抽出されなかった場合（Ｓ’≠Ｓの場合）には、検証局３０は、さらにサーバ端末装置１０からユーザ端末装置２０に送られてきたＥ２（Ｇ＋Ｕ）＋Ｓの情報とそのハッシュ値Ｈ１とその署名との提出をユーザに求め、ハッシュ値Ｈ１とその署名とを確認し、上記ハッシュ値Ｈ１と、Ｅ２（Ｇ＋Ｕ）＋Ｓの情報から生成されるハッシュ値とが一致することを確認する。そして、その確認後に、検証処理の３）の手順でユーザから提出された２次暗号の鍵を用いて上記Ｅ２（Ｇ＋Ｕ）＋Ｓの情報を復号して、電子透かし付き画像データＧｗを取り出す。

【００５５】６）ここで、正しい電子透かし付き画像データが取り出せなかった場合は、ユーザの不正と認定する。これは、上記検証処理中の３）の手順で提出された２次暗号の鍵が正しくないことを意味する。

７）一方、正しい電子透かし付き画像データが取り出せた場合は、サーバの不正と認定する。

以上の検証処理の手順から明らかなように、検証局３０の端末装置は、ユーザ端末装置２０内の２次暗号化処理部２４、２次復号処理部２５、ハッシュ確認処理部２７と同様の処理機能を有している。

【００５６】以上のことにより、本実施形態によれば、サーバとユーザの利害は相反するので両者の結託はありえない。これにより、ユーザが正しい署名情報を埋め込まなかった場合、検証処理によって再現画像からそれが検出されるので、ユーザは不正をすることができない。また、サーバは、ユーザ側での２次暗号化の影響を受けた署名情報を埋め込み処理において知ることはできないので、サーバも不正をすることができない。さらに、検証局は、不正画像が発見されるまでは必要なく、不正画像発見以前に不正を行うことはできない。

【００５７】なお、上記の検証処理の手順が公知で、ユーザとサーバとが互いにその結果を見届けあうならば、検証局はなくても各場合に応じてユーザとサーバの不正は特定することができる。

【００５８】〔第２の実施形態〕近年、電子現金と呼ばれるネットワーク上の通貨が実現されつつある。この電子現金は、通常の現金と同様に所有者の名前が記されないので、匿名性が実現されている。もし、匿名性が実現されない場合、商品の売り手は、電子現金から誰がどの商品を購入したかという情報を知ることができ、ユーザのプライバシーが犯されることになる。このため、上述した電子透かしによる著作者の著作権保護と同様に、ユーザのプライバシー保護の実現は重要である。

【００５９】そこで、この第２の実施形態では、購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには、電子透かしの本来の目的である不正配布者の特定が行えるようにする。これは、

例えば、図２に示すようなシステム２００により実現される。このシステム２００は、上述した第１の実施形態におけるシステム１００と同様の構成としているが、ユーザ端末装置２０には、認証局４０からの匿名公開鍵証明書が与えられる構成としている。

【００６０】通常、署名情報を検査する公開鍵には、その正当性を証明するために認証局と呼ばれる機関による証明書が付されていることが多い。この認証局とは、公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成し、発行する。あるユーザから自分の証明書付き公開鍵を送られた他のユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであるということ）を認証する。このような認証局を運営している組織として、VeriSignやCyberTrustという企業がよく知られている。

【００６１】よって、上述した第１の実施形態で述べた埋め込み処理中の２）の手順においてサーバがユーザの契約情報を署名から確認する場合、図２の認証局４０の証明書付きの公開鍵で確認することが考えられる。しかしながら、この証明書には通常、公開鍵の所有者の名前が記されている。よってこの場合、データの購入時におけるユーザの匿名性は実現されていないことになる。

【００６２】これに対して、公開鍵とその所有者との対応を認証局４０が秘密に保持すれば、公開鍵の証明書に所有者の名前を記さないこともできる。このような匿名性を有する公開鍵の証明書を、以後「匿名公開鍵証明書」と呼び、そのような証明書付きの公開鍵を「証明書付き匿名公開鍵」と呼ぶ。そこで、ユーザ端末装置２０は、上述した埋め込み処理中の１）の手順において、契約情報と一緒に契約情報の署名、および署名情報Ｓを検査するための証明書付き匿名公開鍵を送れば、ユーザはディジタルデータの購入時に自分を匿名にすることができる。

【００６３】よって、サーバ端末装置１０には、利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正コピーの発見時には、その証明書付き匿名公開鍵を認証局４０に示してその公開鍵に対応するユーザを教えてもらうことによって、ユーザを特定することができる。以上のことから、上述した第１の実施形態で述べた埋め込み処理中の１），２）の手順と、検証処理中の１），２）の手順とを以下のように変えることにより、ユーザのディジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【００６４】以下、上記図２のシステム２００における埋め込み処理、および検証処理について具体的に説明する。なお、上記図２のシステム２００において、上記図

１のシステム１００と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略し、異なる部分についてのみ具体的に説明するものとする。また、埋め込み処理の１）、２）と検証処理の１）、２）以外については、上述した第１の実施の形態と同様であるため、その詳細な説明は省略する。

【００６５】[埋め込み処理]

１）まず、ユーザ端末装置２０において、契約生成処理部２１は、認証局４０で発行された証明書付き匿名公開鍵と一緒に、所望の画像データを要求する契約情報をその公開鍵に対応する署名を付けてサーバ端末装置１０に送る。

【００６６】２）次に、サーバ端末装置１０において、契約確認処理部１１は、ユーザの公開鍵を認証局４０の公開鍵によって検査するとともに、契約情報の署名をユーザの匿名公開鍵から確認し、その確認後に、少なくとも契約情報および証明書付き匿名公開鍵の一方から利用者情報Ｕを作成する。そして、第１の電子透かし埋め込み処理部１２により上記契約確認処理部１１で作成された利用者情報Ｕを要求された画像データＧに埋め込んだ後、１次暗号化処理部１３により１次暗号化処理Ｅ１()を行い、得られたデータをユーザ端末装置２０に送る。よって、ユーザ端末装置２０には、１次暗号化画像データＥ１（Ｇ＋Ｕ）の情報が送られる。以降、上述した第１の実施形態における埋め込み処理の３）～５）と同様の処理を行う。

【００６７】[検証処理]

１）サーバ端末装置１０は、発見した不正画像Ｇｗ’から利用者情報Ｕ’を抽出し、その抽出した利用者情報Ｕ’と契約情報から分かる匿名公開鍵とを認証局４０に示し、その匿名公開鍵に対応するユーザ名を聞く。

２）サーバ端末装置１０は、不正画像ＧＷ’と抽出した利用者情報Ｕ’、およびユーザ名を検証局３０に示し、ユーザへの検査を要求する。

そして、上述した第１の実施形態における検証処理の３）～７）と同様の処理を行う。

【００６８】以上述べたように、第２の実施形態によれば、ユーザはディジタルデータの購入時において検証局に対しても匿名性が保つことができる。

【００６９】上述の第１および第２の実施形態に示した画像データ、および透かし情報の埋め込み処理によって得られるハッシュ値を含む種々のデータは、以下のような画像フォーマットで格納することができる。例えば、下記の一般的な画像フォーマットでは、各段階で送付される画像データを画像データ部に格納し、それに対応するハッシュ値やその署名などを画像ヘッダ部に格納することができる。また、最終的にユーザが保存しておく必要があるハッシュ値およびその署名や、２次暗号の鍵等を画像ヘッダ部に、電子透かし付き画像データを画像データ部に格納しておくことができる。

【００７０】一方、下記に示すFlashPixTMファイルフォーマットでは、上記のようなハッシュ値やその署名を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、ハッシュ値やその署名などは、属性情報としてプロパティセットの中に格納しておくこともできる。

【００７１】まず、一般的な画像フォーマットについて説明する。一般的な画像フォーマットでは、図３に示すように、画像ファイルは画像ヘッダ部と画像データ部とに分けられる。

【００７２】一般的に画像ヘッダ部には、その画像ファイルから画像データを読み取るときに必要な情報や、画像の内容を説明する付帯的な情報が格納される。図３の例では、その画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置へのオフセット、カラーパレットのサイズなどの情報が格納されている。一方、画像データ部は、画像データを順次格納している部分である。このような画像フォーマットの代表的な例としては、Microsoft 社のＢＭＰフォーマットや Compuserve社のＧＩＦフォーマットなどが広く普及している。

【００７３】次に、FlashPixTMファイルフォーマットについて具体的に説明する。以後説明するFlashPixTM（FlashPixは米国Eastman Kodak 社の登録商標）ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データ部に格納されていた画像データを、更に構造化してファイル内に格納する。この構造化した画像ファイルを、図４および図５に示す。ファイル内の各プロパティやデータには、ＭＳ－ＤＯＳのディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。上記図４、図５において、影付き部分がストレージで、影なし部分がストリームである。画像データや画像属性情報はストリーム部分に格納される。

【００７４】図４において、画像データは異なる解像度で階層化されており、それぞれの解像度の画像をSubimageと呼び、Resolution０，１，…，ｎで示してある。各解像度の画像に対して、その画像データを読み出すために必要な情報がSubimage Header に、また画像データがSubimage data に格納される。プロパティセットとは、属性情報をその使用目的や内容に応じて分類して定義したものであり、Summary info. Property Set、Image info. Property Set、Image Content Property Set、Extention list property Set がある。

【００７５】[各プロパティセットの説明]Summary info. Property Setは、FlashPix特有のものではなく、Microsoft 社のストラクチャードストレージでは必須のプロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。また、Comp Obj. St

reamには記憶部（Strage）に関する一般的な情報が格納される。

【００７６】Image Content Property Setは、画像データの格納方法を記述する属性である（図６参照）。この属性には、画像データの階層数、最大解像度の画像の幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはＪＰＥＧ圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義などを記述する。Extention list property Set は、上記FlashPixの基本仕様に含まれない情報を追加する際に使用する領域である。さらに、ICC Profile の部分には、ＩＣＣ（International Color Consortium）において規定される色空間変換のための変換プロファイルが記述される。

【００７７】また、Image info. Property Setは、画像データを使用する際に利用できる様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの下記のような情報を格納する。

・ディジタルデータの取り込み方法／あるいは生成方法に関する情報
・著作権に関する情報
・画像の内容（画像中の人物、場所など）に関する情報
・撮影に使われたカメラに関する情報
・撮影時のカメラのセッティング（露出、シャッタースピード、焦点距離、フラッシュ使用の有無など）の情報
・ディジタルカメラ特有の解像度やモザイクフィルタに関する情報
・フィルムのメーカ名、製品名、種類（ネガ／ポジ、カラー／白黒）等の情報
・オリジナルが書物や印刷物である場合の種類やサイズに関する情報
・スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報

【００７８】図５のFlashPix Image View Objectは、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する画像ファイルである。ビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応するために記憶しておく処理係数のセットである。この図５において、Global info. Property Set の部分には、ロックされている属性リストが記述されており、例えば、最大画像のインデックスや最大変更項目のインデックス、最終修正者の情報などが記述される。

【００７９】また、同図において、Source/Result FlashPix Image Object は、FlashPix画像データの実体であり、Source FlashPix Image Objectは必須で、Result FlashPix Image Objectはオプションである。Source FlashPix Image Objectはオリジナルの画像データを、Result FlashPix Image Objectはビューイングパラメータを使って画像処理した結果の画像データをそれぞれ格納する。

【００８０】また、Source/Result desc. Property Setは、上記画像データの識別のためのプロパティセットであり、画像ＩＤ、変更禁止のプロパティセット、最終更新日時等を格納する。Transform Property Setは、画像の回転、拡大／縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【００８１】次に、画像データの取り扱いについて説明する。ここでは、複数のタイルに分割された複数の解像度の画像を含む画像フォーマットを例に挙げて説明する。図７に、解像度の異なる複数の画像から構成される画像ファイルの例を示す。この図７において、最大解像度の画像は列×行がＸ０×Ｙ０で構成されており、その次に解像度の大きい画像はＸ０／２×Ｙ０／２であり、それ以降順次、列・行ともに１／２ずつ縮小し、列・行ともに６４画素以下あるいは互いに等しくなるまで縮小されていく。

【００８２】このように画像データを階層化した結果、画像の属性情報として「１つの画像ファイル中の階層数」や、それぞれの階層の画像に対して、一般的な画像フォーマットの項で説明したヘッダ情報と画像データとが必要となる（図３参照）。１つの画像ファイル中の階層の数や最大解像度の画像の幅、高さ、あるいはそれぞれの解像度の画像の幅、高さ、色構成、圧縮方式等に関する情報は、上記ImageContent Property Set中に記述される（図６参照）。

【００８３】さらに、各解像度のレイヤの画像は、図８に示すように６４画素×６４画素でなるタイル毎に分割されている。画像の左上部から順次６４画素×６４画素のタイルに分割をすると、画像によっては右端および下端のタイルの一部に空白が生ずる場合がある。この場合は、それぞれ最右端画像または最下端画像を繰り返し挿入することで、６４画素×６４画素を構築する。

【００８４】FlashPixTMでは、それぞれのタイル中の画像データをＪＰＥＧ圧縮、シングルカラー、非圧縮のいずれかの方法で格納する。ＪＰＥＧ圧縮は、ISO/IEC JTC1/SC29 により国際標準化された画像圧縮方式であり、方式自体の説明はここでは割愛する。また、シングルカラーとは、上記１つのタイルがすべて同じ色て構成されている場合にのみ、個々の画素の値を記録することなく、そのタイルの色を１色で表現する方式である。この方法は特に、コンピュータグラフィックスにより生成された画像で有効である。

【００８５】このようにタイル分割された画像データは、例えば図４のSubimage data ストリーム中に格納され、タイルの総数、個々のタイルのサイズ、データの開始位置、圧縮方法はすべてSubimage Header に格納されている（図９参照）。

【００８６】〔その他の実施形態〕以上に述べた第１および第２の実施形態において、透かし情報の埋め込み

は、種々の手法によって実現できるが、例えば、「清水，沼尾，森本（日本ＩＢＭ）：“ピクセルブロックによる静止画像データハイディング”，情報処理学会第５３回全国大会，1N-11，平成８年９月」の文献や、「I.J.Cox，J.Kilian，T.Leighton and T.shamoon(ＮＥＣ)：“Sucure Spread Spectrum Watermarking forMultimedia，”ＮＥＣ Reserch Institure Technical Report 95-10.」の文献に示されるような公知の埋め込み手法によって実現できる。

【００８７】また、１次暗号，２次暗号として用いられる暗号方式も種々の方式によって実現できるが、例えばビットの配置を暗号鍵に応じて換えるといった暗号方式によって実現できる。また、全ての送信データにハッシュ値とその署名を付けて送ることもできる。さらに、１次暗号と２次暗号は、透かし情報の埋め込み処理においてサーバ側とユーザ側とで互いの情報を知らせないために用いられるが、第三者からの通信路上での盗聴および改ざんを防ぐために、別にＤＥＳ（Data Encryption Standard）等の暗号やハッシュ関数等を用いても良い。

【００８８】また、上述の第１および第２の実施形態において、不正配布の検出はサーバ側が行っているが、１次暗号または２次暗号に関する秘密鍵を知らなくても電子透かしの抽出手段さえ持っていれば、誰にでも不正配布および不正配布の利用者情報を知ることができる。その後、不正配布発見をサーバ側に知らせて検証処理を始めさせれば良いので、不正配布の発見者はサーバに限定されない。

【００８９】また、サーバ端末装置１０は、利用者情報Ｕだけでなく、必要に応じて著作権情報やその画像データの配布状況に関する情報等の他の情報を画像データに埋め込むこともできる。また、サーバ端末装置１０で秘密の情報を埋め込みたい場合は、１次暗号化の後に埋め込み処理を行えば、署名情報と同様に１次暗号の影響を受けた情報を埋め込むことができる。さらに、利用者情報Ｕは、必ず１次暗号化の前にある必要はなく、１次暗号化の後に埋め込んでもよい（この場合、利用者情報Ｕの検出は、サーバまたは１次暗号の秘密鍵を知る者のみが行える）。

【００９０】また、ユーザが複数のユーザ間で共通のプリンタや端末等を用いるユーザである場合、ユーザの署名情報および２次暗号は、プリンタや共通端末の署名情報や暗号方式を含む場合がある。また、サーバ端末装置１０からの１次暗号化情報は、ユーザ端末装置２０からの契約情報による依頼がなくても、ネットワークやＣＤ－ＲＯＭ等によって広く配布されていても良い。

【００９１】また、ユーザの署名情報Ｓは、公開鍵暗号方式によって生成されなくても、ユーザが契約情報等で定めた情報（暗証番号のような情報）等でも良い。また、米国では４０ビット以上の暗号を用いる場合、暗号の悪用を防ぐために暗号鍵を管理する鍵管理局を必要とする。そこで、検証局３０に鍵管理局を兼ねさせることも可能である。よって、検証局３０が２次暗号の鍵をあらかじめ管理している場合には、不正画像の監視も検証局３０が行えば、検証処理１）～３）は検証局３０が単独で行うことができる。サーバ端末装置１０での１次暗号の鍵は、同じ検証局３０によって管理されていてもよいし、他の鍵管理局によって管理されていてもよい。また、サーバ端末装置１０やユーザ端末装置２０の鍵は、鍵管理局が生成し、配布してもよい。

【００９２】

【発明の効果】上述の説明から明らかなように、本発明の電子透かし方式および電子情報配布システムによれば、ディジタルデータを不正にコピーして配布を行った際にその不正行為および不正行為者を確実に認識することができ、これによって不正を確実に防止することが可能となり、ディジタルデータの不正配布に関して安全なシステムを実現することができる。また、上記電子透かし方式を用いて電子透かしを埋め込んだ画像データをファイルできる画像ファイル装置で、特に埋め込まれた電子透かし情報を比較的容易に確認することのできる画像ファイル装置を得ることができる。さらに、このシステムによってユーザの匿名性や暗号の悪用を防ぐ鍵管理局への応用も容易に実現できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を示した電子透かしシステムを説明するための図である。

【図２】本発明の第２の実施形態を示した電子透かしシステムを説明するための図である。

【図３】一般的な画像フォーマットを示す図である。

【図４】FlashPixTMファイルフォーマットの例を示す図である。

【図５】FlashPixTMファイルフォーマットの例を示す図である。

【図６】FlashPixTMファイルフォーマットのImage Content Property Setに格納される属性情報を示す図である。

【図７】それぞれ解像度の異なる複数の画像から構成される画像ファイルの例を示す図である。

【図８】各解像度のレイヤの画像のタイル分割の様子を示す図である。

【図９】タイル分割された画像データに関する属性情報を示す図である。

【図１０】従来の電子透かしシステムを説明するための図である。

【図１１】図１０に示す方式を改良した従来の電子透かしシステムを説明するための図である。

【図１２】図１１に示す方式を改良した従来の電子透かしシステムを説明するための図である。

【符号の説明】

１０　サーバ端末装置

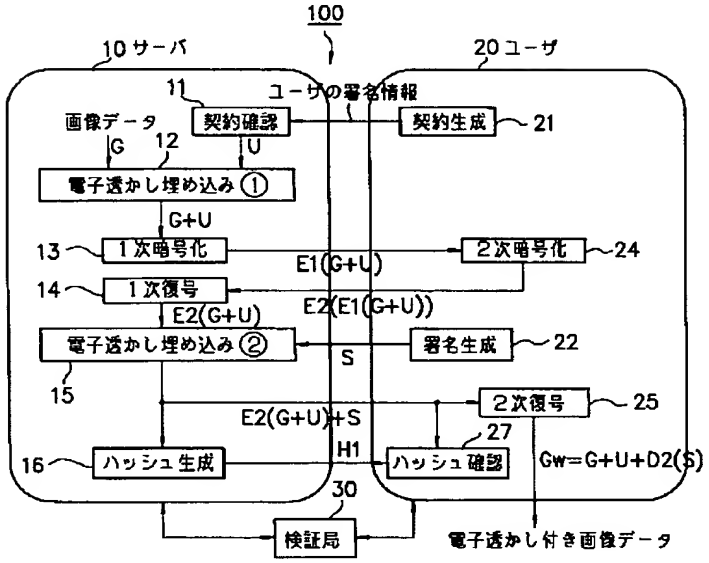
21

１１　契約確認処理部
１２　第１の電子透かし埋め込み処理部
１３　１次暗号化処理部
１４　１次復号処理部
１５　第２の電子透かし埋め込み処理部
１６　ハッシュ生成処理部
２０　ユーザ端末装置
２１　契約生成処理部

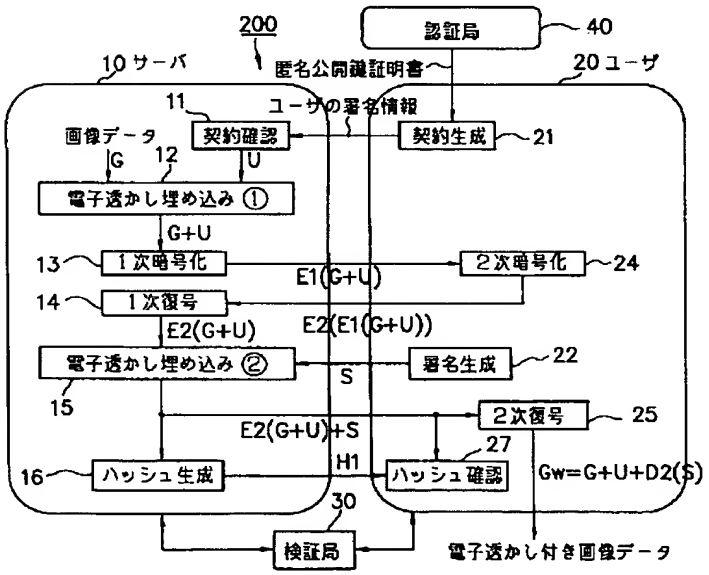
22

２２　署名生成処理部
２４　２次暗号化処理部
２５　２次復号処理部
２７　ハッシュ確認処理部
３０　検証局端末装置
４０　認証局端末装置
１００　電子情報配布システム
２００　電子情報配布システム

【図１】



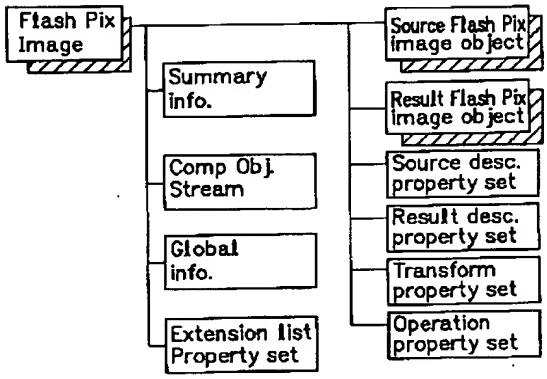
【図２】



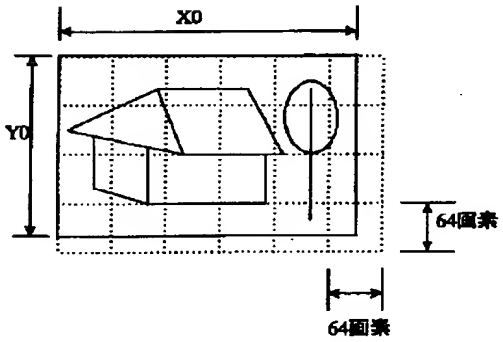
【図３】

画像ヘッダ部	画像フォーマット識別子
	ファイルサイズ
	X方向ピクセル数（幅）
	Y方向ピクセル数（高さ）
	深さ方向サイズ
	圧縮の有無
	解像度
	ビットマップへのオフセット
	カラーパレットサイズ
画像データ部	ビットマップ

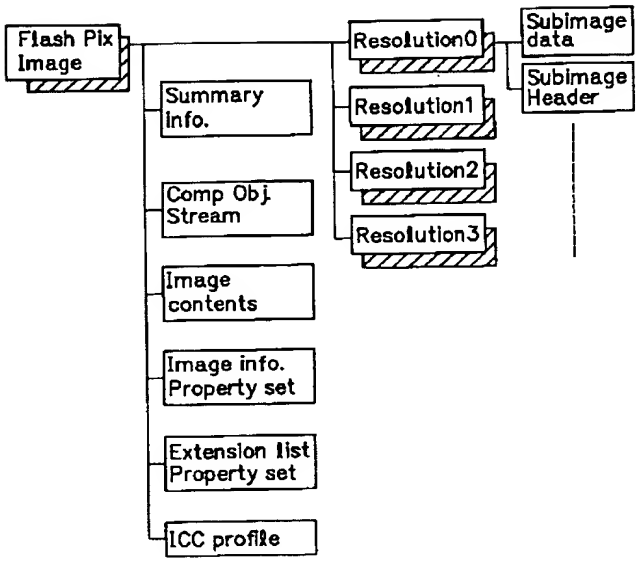
【図５】



【図８】



【図４】



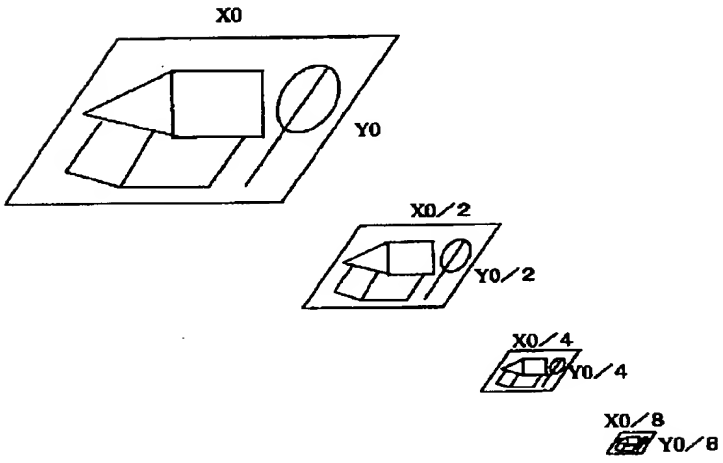
【図６】

プロパティ名	ＩＤコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

プロパティ名	ＩＤコード	タイプ
各解像度の画像の幅	0x02ii0000	VT_UI4
各解像度の画像の高さ	0x02ii0001	VT_UI4
各解像度の画像の色	0x02ii0002	VT_BLOB
各解像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4|VT_VECTOR

プロパティ名	ＩＤコード	タイプ
ＪＰＥＧテーブル	0x03ii0001	VT_BLOB
最大ＪＰＥＧテーブルのインデックス	0x03000002	VT_UI4

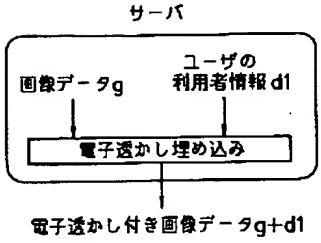
【図７】



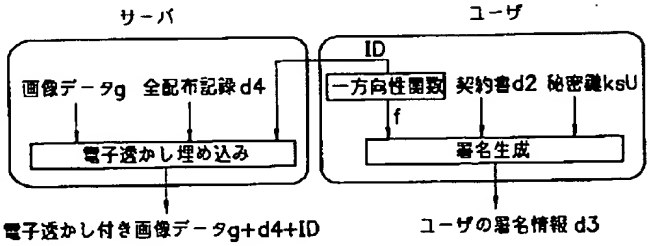
【図９】

フィールド名	長さ	バイト
画像の幅	4	4−7
画像の高さ	4	8−11
タイルの総数	4	12−15
タイルの幅	4	16−19
タイルの高さ	4	20−23

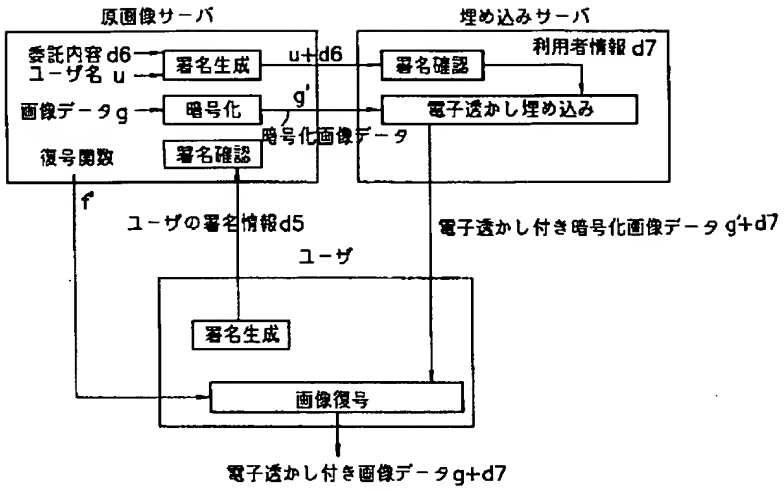
【図１０】



【図１１】



【図１２】



フロントページの続き

(51) Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｄ
Ｈ０４Ｎ	7/08		Ｈ０４Ｎ	7/08	Ｚ
	7/081				